FORM PTO-1390 (REV. 5-93)	U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEY'S DOCKET NUMBER **2345/45**

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
To be assigned 09/202024

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP97/02894	**20 December 1997 (20.12.97)**	**05 June 1996 (05.06.96)**

TITLE OF INVENTION
METHOD AND DEVICE FOR LOADING INPUT DATA INTO AN ALGORITHM WHEN PERFORMING AN AUTHENTICATION

APPLICANTS FOR DO/EO/US SCHAEFER-LORINSER, Frank and SCHEERHORN, Alfred

Applicants herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). Unexecuted.
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1 98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: PCT/RO/101 Request Form.

45556-1
Express Mail No. EL169613221US

U.S. APPLICATION NO if known, see 37 C.F.R.1 5	INTERNATIONAL APPLICATION NO. PCT/EP97/0289	ATTORNEY'S DOCKET NUMBER 2345/45

17. ☒ The following fees are submitted:

	CALCULATIONS	PTO USE ONLY
Basic National Fee (37 CFR 1.492(a)(1)-(5)): Search Report has been prepared by the EPO or JPO $930.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) . . . $720.00		
No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) $790.00		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO $1,070.00		
International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) $98.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 930.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$ 0	

Claims	Number Filed	Number Extra	Rate		
Total Claims*	15 - 20 =	0	X $22.00	$ 0	
Independent Claims	2	0	X $82.00	$ 0	
Multiple dependent claim(s) (if applicable)			+ $270.00	$ 0	
*based on Preliminary Amendment		**TOTAL OF ABOVE CALCULATIONS =**		$930.00	
Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28).				$ 0	
		SUBTOTAL =		$930.00	
Processing fee of $130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +				$ 0	
		TOTAL NATIONAL FEE =		$930.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3 28, 3.31). $40.00 per property +				$ 0	
		TOTAL FEES ENCLOSED =		$930.00	
*Calculations based on Preliminary Amendment.				Amount to be: refunded	$
				charged	$

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of **$930.00** to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Richard L. Mayer

By: Mary C. Werner

Richard L. Mayer (Reg. No. 22,490)

Reg. No. 30,333

DATE 12/4/98

KENYON & KENYON
One Broadway
New York, NY 10004

[2345-45]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: SCHAEFER-LORINSER et al.

SERIAL NO.: to be assigned

FILED: herewith

TITLE: METHOD AND DEVICE FOR LOADING INPUT DATA INTO A PROGRAM WHEN PERFORMING AN AUTHENTICATION, Originally filed in PCT as "METHOD AND DEVICE FOR LOADING INPUT DATA INTO AN ALGORITHM WHEN PERFORMING AN AUTHENTICATION"

ART UNIT: not yet known

EXAMINER: not yet known

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

PRELIMINARY AMENDMENT

Please amend the above-identified application before a first consideration on the merits as follows:

IN THE TITLE

Change "AN ALGORITHM" to --A PROGRAM--.

IN THE DRAWINGS

Please add new Fig. 1.

IN THE SPECIFICATION

On page 1, before line 1, please insert --Field of the Invention.

On page 1, line 1, between "The" and "invention" insert --present--, and change "to a method as described in detail in the preamble to Claim 1," to --generally to a method for loading input data into a program when performing an authentication, and, in particular, to a

EL169613221US

method for loading input data into a program when performing an authentication between electronic cash cards and a security module.--.

On page 1, delete line 2.

On page 1, before line 3, insert --Related Technology

Various prior--.

On page 1, line 3, delete "of this kind" and delete "and".

On page 1, line 4, change "the devices are based, inter alia, on" to --with devices being based on, among other things,-- and change "EP" to --European Patent Application Number--.

On page 1, line 6, change "Methods of the kind referred to here are known" to --Related methods are described-- and change "from" to --in--.

On page 1, line 17, change "EP" to --European Patent Application Number--.

On page 1, line 19, change "locations" to --areas--.

On page 2, line 2, change "(P95114) proposed a method whereby" to --in a method described in PCT Patent Application Number 95114--.

On page 2, line 4, change "machine and, during" to --machine. During--.

On page 2, line 7, change "balance; after that" to --balance. Subsequently,--.

On page 2, line 8, change "made; and finally" to --made. Finally--.

On page 2, line 11, change "module; following" to --module. Following--.

On page 2, before line 14, insert --Summary of the Invention--.

On page 2, line 14, change "The object" to --An object--.

On page 2, line 15, change "the 'electronic cash purses'" to --electronic cash cards.--

On page 2, before line 18, insert --The present invention therefore provides a method for loading input data into an algorithm when performing a cash transaction authentication between an electronic cash chip card and a security module.

Brief Description of the Drawings

The present invention may be more easily understood with reference to the drawing, in which:

Fig. 1 shows a block diagram of a method in accordance with the present invention.

Detailed Description

Fig. 1 shows a block diagram of the method of the present invention for loading input data into a program when performing a cash transaction authentication between an electronic cash chip card and a security module, the chip card including a stored credit balance. As shown in block 102, a cash amount requested, preferably input by the cardholder, is debited from an electronic cash chip card using a security function. The requested cash amount is added and stored in a cash amount summing counter of a security module, as shown in block 104. Then, as shown in block 106, input data is subdivided into a plurality of data blocks. According to the present invention, the data blocks are loaded into a linear-feedback shift register for performing the program, the linear-feedback shift register having at least one non-linear function cryptographically enhanced using at least one downstream counter, as shown in block 108. Next, at least one additional feedback is introduced into the linear-feedback shift register following the at least one downstream counter, as shown in block 110. Lastly, as shown in block 112, the at least one additional feedback is switched off after a predefined number of clock pulses.--

On page 2, delete lines 18-30.

On page 3, line 3, delete "as well,".

On page 3, line 6, delete "the".

On page 3, line 11, change "the condition being" to --where it is required--.

On page 3, line 18, change "can" to --may-- and change "in that" to --with--.

On page 3, line 19, change "are" to --being-- and change "functions' =" to --functions," that is,--.

On page 3, line 21, change "can" to --may--.

On page 3, line 23, between "then" and "be" insert --may--.

On page 3, line 24, change "strong enough" to --sufficiently powerful--.

On page 3, line 26, change "insofar as" to --in that--.

On page 4, line 1, change "The" to --An--.

On page 4, line 8, change "used:" to used. Exemplary steps and features include:--.

On page 4, line 5, change "0. Additional" to ---Additional--.

On page 4, line 8, change "1. Input" to ---Input--.

On page 4, line 13, change "2. A" to ---A--.

On page 4, line 16, change "3. Input" to ---Input--.

On page 4, line 19, change "4. The" to ---The--.

On page 4, line 22, change "5. A" to ---A--.

On page 5, line 1, change "Patent Claims" to --WHAT IS CLAIMED IS:--.

IN THE CLAIMS

Please delete claims 1-14 and add new claims 15-29 as follows:

-- 15. (new) A method for loading input data into a program when performing a cash transaction authentication between an electronic cash chip card and a security module, the chip card including a stored credit balance, the method comprising:

debiting a requested cash amount from the chip card using a security function;

adding and storing the requested cash amount in a cash amount summing counter of the security module,

subdividing the input data into a plurality of data blocks;

loading the plurality of data blocks into a linear-feedback shift register for performing the program, the linear-feedback shift register having at least one non-linear function cryptographically enhanced using at least one downstream counter;

introducing at least one additional feedback into the linear-feedback shift register following the at least one downstream counter; and

switching off the at least one additional feedback after a predefined first number of pulses of an associated clock.

16. (new) The method as recited in claim 15 wherein the input data includes at least a random number, a secret key, and non-secret chip card data.

17. (new) The method as recited in claim 15 wherein the input data includes at least a random number, a secret key, and non-secret chip card data, the secret key being associated with the non-secret chip card data, the input data being subdivided so that the non-secret chip card data and the secret key form a first data block and the random number forms a second data block.

18. (new) The method as recited in claim 15 wherein different contents of the at least one downstream counter are used during the loading step than are used after the loading step in calculating an authentication token.

19. (new) The method as recited in claim 15 wherein a first downstream counter of the at least one downstream counter counts to 1.

20. (new) The method as recited in claim 15 wherein the at least one downstream counter and the first number of clock pulses are selected so as to enable calculating of an authentication token to be based on a second number of clock pulses.

21. (new) The method as recited in claim 15 further comprising outputting bits after the loading is completed.

22. (new) The method as recited in claim 15 wherein the linear-feedback shift register forms at least part of a circuit, and further comprising:

outputting bits after the loading of the blocks is completed; and

pulsing the circuit for a third number of pulses of the clock while maintaining the at least one additional feedback between the loading of the blocks and the outputting of the bits.

23. (new) The method as recited in claim 15 wherein the linear-feedback shift register forms at least part of a circuit, and further comprising:

outputting bits after the loading of the blocks is completed;

switching off the at least one additional feedback; and

pulsing the circuit for a third number of pulses of the clock after the switching off of the at least one additional feedback

24. (new) A device for loading input data into a program when performing an authentication using a cryptographic MAC function, the device comprising:

a first counter;

a linear-feedback shift register having a nonlinear feed-forward function for reading off from the linear-feedback shift register, and for influencing an output of the linear-feedback shift register using the counter, the linear-feedback shift register forming at least part of a circuit;

at least one second counter for performing the program, the at least one second counter connected downstream of the linear-feedback shift register; and

at least one additional non-linear feedback for cryptographically enhancing the circuit, the at least one additional nonlinear feedback shift register being disconnectable.

25. (new) The device as recited in claim 24 further comprising a latch, and wherein the additional feedback is tapped off following a first of the at least one second downstream counter and before the latch.

26. (new) The device as recited in claim 24 further comprising a latch, and wherein the additional feedback is read off from the latch following a first of the at least one second downstream counter.

27. (new) The device as recited in claim 24 wherein the additional feedback is read off following a second of the at least one second downstream counter.

28. (new) The device as recited in claim 24 further comprising a latch, and wherein the additional feedback is generated as an XOR sum of readouts following a first of the at least one second downstream counter before the latch, from the latch following the first of the at least one second downstream counter, and following a second of the at least one second downstream counter.

29. (new) The device as recited in Claim 24, wherein the first counter and the at least one second counter are subdivided or reduced.--

IN THE ABSTRACT

In the title, change "Abstract of the Disclosure" to --Abstract--.

Line 1, change "2.1. The problems posed by" to --A method for enhancing--.

Line 2, change "are encountered when" to --and--.

Line 5, delete "2.2."

Line 7, change "times (clock pulses)" to --clock pulse times--.

Line 9, change "2.3. The invention" to --The method--.

REMARKS

This Preliminary Amendment cancels original claims 1-14 in the underlying PCT Application No. PCT/EP97/02894, and adds new claims 15-29. The new claims do not add new matter to the application but do conform the claims to U.S. Patent and Trademark Office rules.

The amendments to the specification and abstract are to conform the specification and abstract to U.S. Patent and Trademark Office rules. The new figure, as well as the amendments to the specification and abstract, does not introduce new matter into the application.

Conclusion

Consideration of the present application as amended is hereby respectfully requested.

Respectfully Submitted,

Dated: 1 December 1998

Erik R. Swanson
(Reg. No. 40,833)

1 Broadway
New York, NY 10004
(212) 425-7200

[2345/45]

Method and Device for Loading Input Data into an Algorithm When Performing an Authentication

The invention relates to a method as described in detail in the preamble to Claim 1, and to a device of the kind defined in the preamble to Claim 9. Various known methods of this kind are used for electronic cash cards in a plurality of variants, and the devices are based, inter alia, on chip circuits as described by EP 0 616 429 Al.

Methods of the kind referred to here are known, for example, from ETSI D/EN/TE 090114, Terminal Equipment (TE) Requirements for IC Cards and Terminals for Telecommunication Use, Part 4 - Payment Methods, version 4, of February 7, 1992, and from the European Patent Application 0 605 070.

In addition to phone cards, which have a defined initial credit balance as a payment means for card-operated phones, "electronic cash cards", which work according to the same principle, are gaining in significance as a means for paying limited amounts. In "pay with chip card" applications, a card reader module having a security module SM for verifying the card and the balance amount are integrated in the automatic machine.

EP 0 605 070 A2 also describes a method for transferring credit and debit amounts to and from chip cards, memory locations of a chip card having overwrite capability being divided into at least two memory locations, one of these having a "debit function", thus acting as an "electronic purse" similarly to a phone card, and the other having a "credit function" along the lines of a credit card. To replenish the "electronic purse", provision is made for cash amounts to be transferred between the areas under the secured conditions that are typical for credit cards.

To both avoid the danger of unauthorized access to the automatic teller machines and their permanently installed security modules, as well as eliminate the need for

dedicated lines which are specially protected and, thus, expensive for the operator, (P95114) proposed a method whereby, prior to any cash transaction, the operator of the automatic cash machine inserts a security module having chip card functions into the automatic cash machine and, during each cash transaction that involves a cardholder inserting his or her electronic cash card into an automatic cash machine, data areas of the chip card are first read out to permit a plausibility check and to verify the remaining credit balance; after that, an authentication is performed using the security module and a single or multiple acceptance decision is made; and finally, the cash amount due or input is either debited to the cardholder's chip card with the aid of a security function, or added to a summing counter for cash amounts in the security module; following the cash transactions, the counter content of the security module having chip card functions is transferred to a clearinghouse.

The object of the present invention is to further enhance the security of automatic cash machines for the "electronic cash purses" to prevent unauthorized manipulation and malfunctions.

This object is achieved in accordance with the characterizing part of Claim 1.

Advantageous variants or further developments of this method are described in the characterizing parts of dependent Claims 2 through 8.

The characterizing part of Claim 9 describes a device which is suitable for the application of the method.

The characterizing parts of dependent Claims 10 through 14 contain advantageous variants or further developments of these devices for various applications.

The invention, including its effects, advantages and fields of application, is described in detail by the following examples.

Authentication algorithms are typically used to enable reliable identification. Often entering into the authentication methods, besides the identity of a chip card, of a person, and possibly of a security module SM, are other data, as well, which have to be verified. An authentication method can be applied, for example, to non-secret card data D, together with a secret key K, and a random number Z. For the sake of security when working with the electronic cash cards, separate security functions are used for debiting and crediting, and each of these security functions is retrieved using a cryptographic checksum.

The method of the present invention enables the debit and credit transactions to be carried out using a cryptographic token, the condition being that the authentication and cryptographic checksum process are performed on the counter content using a challenge/response method. A single challenge/response method can then be applied, whereby only one random number is provided by the security module SM and only one response is calculated by the chip card, to verify both the identity (authentication) as well as the internal counter content with respect to the security module SM.

This can be achieved in that the variable input data, such as the counter content and the random number, are initially processed internally using "keyed hash functions" = MAC functions. In the process, the card-specific secret key of the chip card is used as the key. The two tokens extracted from counter content and the random number can then be linked together, for example, (in a perhaps cryptographically unsecured way) by XOR or by using a linear-feedback shift register, and then be output, with their integrity being protected, using a cryptographic function that is strong enough.

This method is of practical use insofar as the keyed hash functions, which are only used internally, do not have to meet any particularly high requirements with regard to their security, and relatively simple functions can be used since the results of these functions do not leave the chip card. Nevertheless, data manipulation is effectively prevented with this method.

The exemplary embodiment of the present invention assumes that a linear-feedback shift register (LFSR) having an additional nonlinear function and downstream counters is used:

0. Additional feedback circuits are switched into the linear-feedback shift register LFSR following the downstream counters.

1. Input data, composed of the non-secret card data D and the secret key K, are read into the linear-feedback shift register LFSR, while both the feedback of the linear-feedback shift register LFSR, as well as the additional feedback(s) are active.

2. A certain number of clock pulses is processed without additional input data being read in.

3. Input data made up of the random number R are read in while both the feedback of the LFSR and the additional feedback(s) are active.

4. The additional feedback circuits are switched off, and the counters are reset, if necessary.

5. A certain number of clock pulses is processed, and, during these pulses, output bits are generated according to the current counter settings.

Patent Claims

1. A method for loading input data into an algorithm when performing an authentication between electronic cash cards and a security module, where the cardholder may have a stored credit balance available to him or her, and where, for every cash transaction, the cash amount requested or input by the cardholder is debited from the cardholder's chip card with the aid of a security function, and the cash amounts are added and stored in a summing counter for cash amounts of the security module, and where for the authentication algorithm, a linear-feedback shift register is used, whose non-linear functions are cryptographically enhanced in conjunction with downstream counters, and where input data, such as a random number, a secret key, and non-secret card data, enter into this algorithm,
wherein input data are subdivided into a plurality of blocks of data, and while the blocks are loaded into the linear-feedback shift register, an additional, further feedback is introduced into the shift register following the downstream counter and is switched off following a predefined number of clock pulse steps.

2. The method as recited in Claim 1,
wherein the card data D having a secret key K are introduced as a first block, and a random number R is introduced as an additional block.

3. The method as recited in Claim 1 and 2,
wherein during the phase in which the input data are loaded, other counter contents are used than during the subsequent phase after the input data are loaded to calculate the authentication token.

4. The method as recited in Claim 1 and 2,
wherein the first downstream counter counts to 1.

5. The method as recited in Claim 1 and 2,
wherein the counter and the number of clock pulses to be implemented are selected with precision so as to ensure that the authentication token is calculated based on a number of clock pulses that is fixed by other system conditions.

6. The method as recited in one of Claims 1 through 5,
wherein the outputting of bits begins after all input data have been loaded.

7. The method as recited in one of Claims 1 through 6,
wherein in the time between the loading of the blocks from Claim 1 and the outputting of the bits, the entire circuit continues to be pulsed for several clock pulses while the additional feedback is maintained, without input data being loaded.

8. The method as recited in one of Claims 1 through 6,
wherein in the time between the loading of the blocks from Claim 1 and the outputting of the bits, the entire circuit continues to be pulsed for a certain number of clock pulses after the additional feedback is switched off, without input data being loaded.

9. A device for loading input data into an algorithm when performing an authentication using a cryptographic MAC function, made up of a linear-feedback shift register having a nonlinear "feed-forward" function, which reads off from the shift register and, using a counter, influences the output of the shift register, to which an additional counter is connected downstream, wherein the circuit, which is produced from the linear-feedback shift register and which has downstream counters to be used for the authentication algorithm, is cryptographically enhanced by an additional, disconnectable non-linear feedback.

10. The device as recited in Claim 9, wherein the additional feedback is tapped off following the first downstream counter before the latch.

11. The device as recited in Claim 9, wherein the additional feedback is read off from the latch following the first downstream counter.

12. The device as recited in Claim 9, wherein the additional feedback is read off following the second downstream counter.

13. The device as recited in Claim 9, wherein the additional feedback is generated as an XOR sum of the readouts following the first downstream counter before the latch, from the latch following the first downstream counter, and following the second downstream counter.

14. The device as recited in Claim 9, wherein the counters are subdivided or reduced.

Abstract of the Disclosure

2.1. The problems posed by data security when chip cards are used for payment transactions are encountered when input data are loaded into an algorithm when performing an authentication.

2.2. The security of the debit and credit data is enhanced by subdividing the data blocks and by switching an additional feedback on and off following the downstream counters at preselected times (clock pulses).

2.3. The invention is applicable to all authentication processes in conjunction with chip cards.

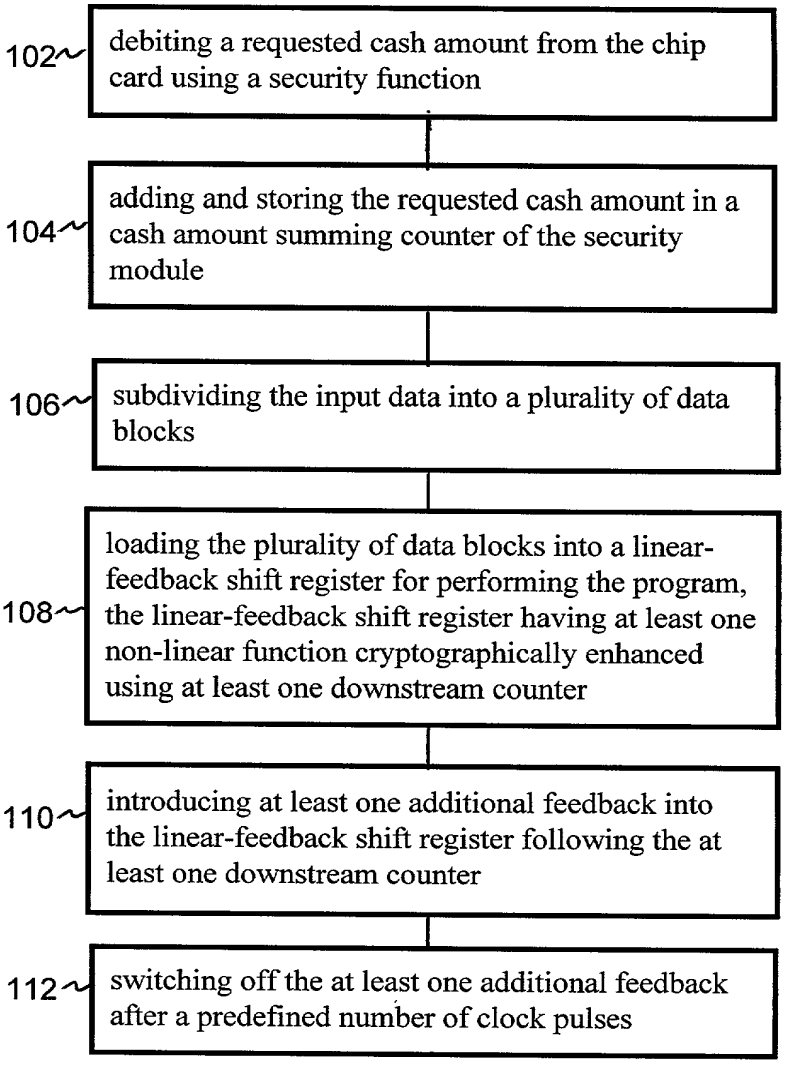

FIG. 1

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

DECLARATION AND POWER OF ATTORNEY	ATTORNEY'S DOCKET NO. 2345/45

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name,

I believe I am an original, first, and joint inventor of the subject matter that is claimed and for which a patent is sought on the invention entitled **METHOD AND DEVICE FOR LOADING INPUT DATA INTO AN ALGORITHM WHEN PERFORMING AN AUTHENTICATION**, the specification of which was filed as International Application No. PCT/EP97/02894 on June 4, 1997.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

PRIOR FOREIGN APPLICATION(S)

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE OF FILING (day, month, year)	DATE OF ISSUE (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. § 119
GERMANY	**196 22 533.7**	**5 June 1996**		**YES**

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorneys:
Richard L. Mayer (Reg. No. 22,490)
William C. Gehris (Reg. No. 38,156)
Erik R. Swanson (Reg. No. 40,833)

SEND CORRESPONDENCE, AND DIRECT TELEPHONE CALLS TO:

Richard L. Mayer
KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200 (phone)
(212) 425-5288 (facsimile)

EL 179958567 US

I declare that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful statements may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR	FAMILY NAME **SCHAEFER-LORINSER**	FIRST GIVEN NAME **Frank**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-64372 Ober-Ramstadt**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Potsdamer Str. 88**	CITY **D-64372 Ober-Ramstadt**	STATE & ZIP CODE/COUNTRY **Germany**
Signature Frank Schaefer-Lorinser		Date 12. april 1999	
FULL NAME OF INVENTOR	FAMILY NAME **SCHEERHORN**	FIRST GIVEN NAME **Alfred**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-49716 Meppen**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Ahornallee 3**	CITY **D-49716 Meppen**	STATE & ZIP CODE/COUNTRY **Germany**
Signature		Date	

I declare that all statements made herein of my own knowledge are true and all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful statements may jeopardize the validity of the application or any patent issuing thereon.

FULL NAME OF INVENTOR	FAMILY NAME **SCHAEFER-LORINSER**	FIRST GIVEN NAME **Frank**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-64372 Ober-Ramstadt**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Potsdamer Str. 88**	CITY **D-64372 Ober-Ramstadt**	STATE & ZIP CODE/COUNTRY **Germany**
Signature		Date	
FULL NAME OF INVENTOR	FAMILY NAME **SCHEERHORN**	FIRST GIVEN NAME **Alfred**	SECOND GIVEN NAME
RESIDENCE & CITIZENSHIP	CITY **D-49716 Meppen**	STATE OR FOREIGN COUNTRY **Germany**	COUNTRY OF CITIZENSHIP **Germany**
POST OFFICE ADDRESS	POST OFFICE ADDRESS **Ahornallee 3**	CITY **D-49716 Meppen**	STATE & ZIP CODE/COUNTRY **Germany**
Signature Alfred Scheerhorn		Date 03.04.1999	